Technical Cybersecurity

Attack Vectors

A single attack vector is a single way to get into a system.

Case: /bin/ls

Let’s start with /bin/ls on MacOS, a commonly used command to list directory contents on Unix systems.

Case: /bin/ls

Vector 0: Environment variables

- LSCOLORS, CLICOLOR, LS_COLWIDTHS, TERM, TZ, etc.

Vector 1: Libraries

- MacOS: libutil.dylib, libncurses.5.4.dylib, libSystem.B.dylib

Vector 2: Command line options

- Umm, yeah, lots of these

Vector 3: Filesystem

- lots of calls through libSystem.B.dylib

(The whole collection is the *attack surface*)

Let’s look at LSCOLORS.

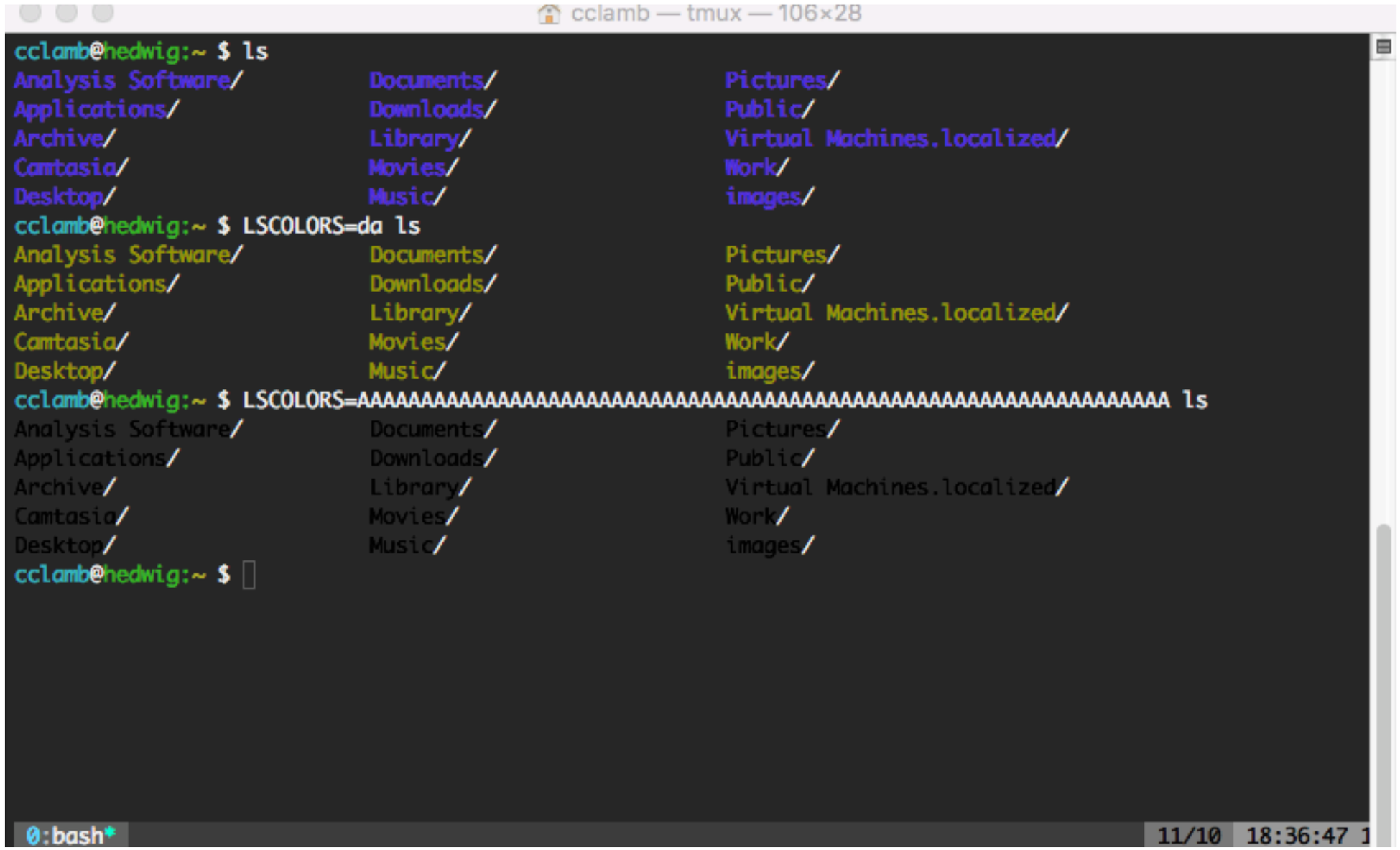
So what is it?

$ MAN LS

- Gives you interesting info
- So LSCOLORS is read by **ls** when the program runs

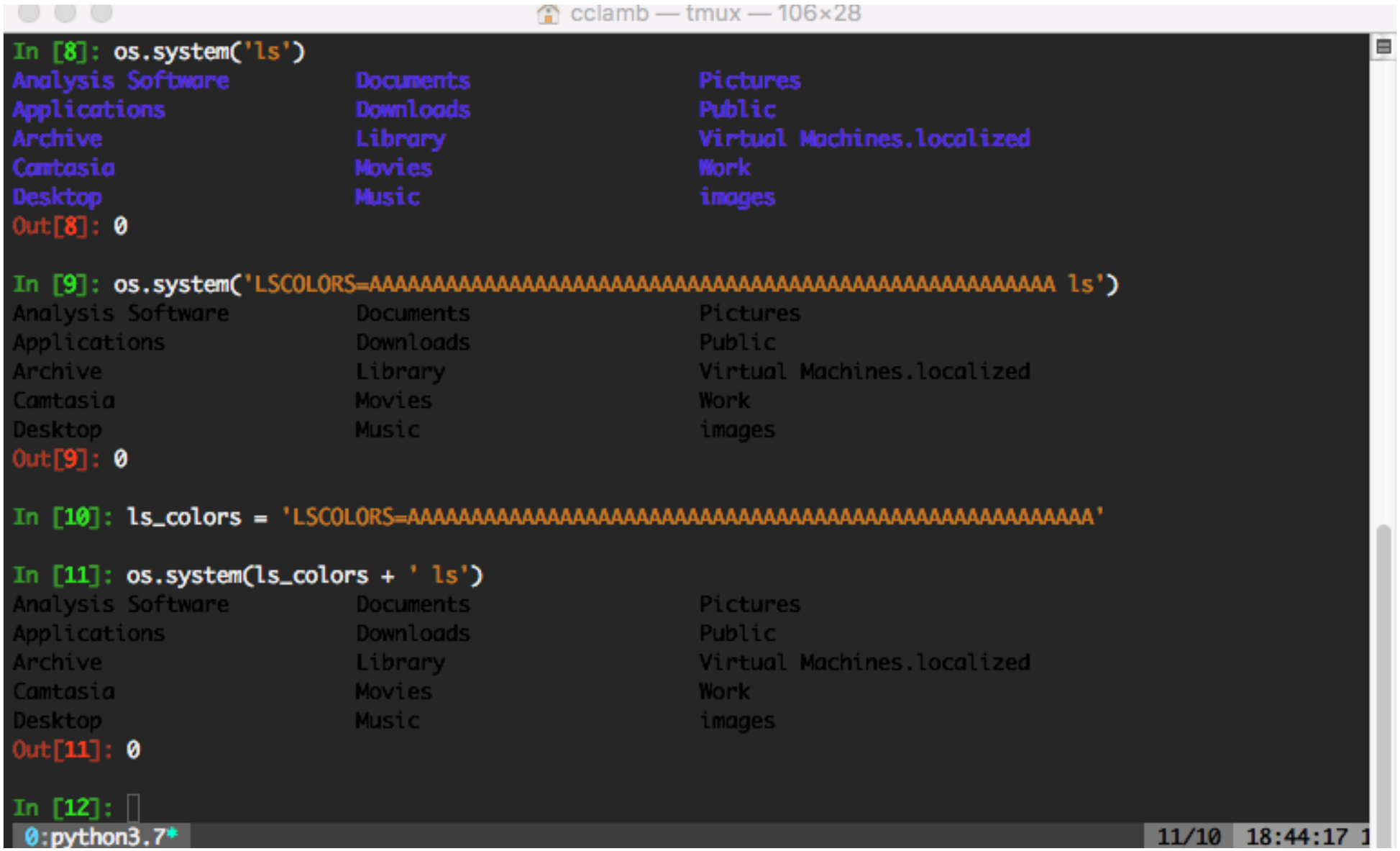
Buffers checked?

```
LSCOLORS        The value of this variable
                describes what color to use
                for which attribute when col-
                ors are enabled with CLICOLOR.
                This string is a concatenation
                of pairs of the format fb,
                where f is the foreground
                color and b is the background
                color.

                The color designators are as
                follows:

                     a     black
                     b     red
                     c     green
                     d     brown
                     e     blue
                     f     magenta
                     g     cyan
                     h     light grey
                     A     bold black, usu-
                           ally shows up as
                           dark grey
                     B     bold red
                     C     bold green
                     D     bold brown, usu-
                           ally shows up as
```



LSCOLORS

Hmmmmm.



Let’s try it in Python!

Usually use subprocess module, but it doesn’t really do what we need wrt LSCOLORS here.

cclamb — tmux — 106×28

```
In [25]: def make_ls_colors():
    ...:     ls_colors = 'LSCOLORS='
    ...:     for i in range(5000):
    ...:         ls_colors = ls_colors + 'A'
    ...:     return ls_colors

In [26]: cols = make_ls_colors()

In [27]: os.system(cols + ' ls')
Analysis Software          Documents                  Pictures
Applications               Downloads                  Public
Archive                    Library                    Virtual Machines.localized
Camtasia                   Movies                     Work
Desktop                    Music                      images
Out[27]: 0

In [28]:
```

0:python3.7* 11/10 18:49:15 1

Try it out!

You get the idea. Now try other things!

Why do I care about attack surfaces?